

# Innovative Instructions and Software Model for Isolated Execution

Frank McKeen ([frank.mckeen@intel.com](mailto:frank.mckeen@intel.com)),  
Ilya Alexandrovich ([ilya.alexandrovich@intel.com](mailto:ilya.alexandrovich@intel.com)),  
Alex Berenzon ([alex.berenzon@intel.com](mailto:alex.berenzon@intel.com)),  
Carlos V Rozas ([carlos.v.rozas@intel.com](mailto:carlos.v.rozas@intel.com)),  
Hisham Shafi ([hisham.shafi@intel.com](mailto:hisham.shafi@intel.com)),  
Vedvyas Shanbhogue ([vedvyas.shanbhogue@intel.com](mailto:vedvyas.shanbhogue@intel.com)),  
Uday R Savagaonkar ([uday.r.savagaonkar@intel.com](mailto:uday.r.savagaonkar@intel.com))

## Abstract:

For years the PC community has struggled to provide secure solutions on open platforms. Intel has developed innovative new technology to enable SW developers to develop and deploy secure applications on open platforms. The technology enables applications to execute with confidentiality and integrity in the native OS environment. It does this by providing ISA extensions for generating hardware enforceable containers at a granularity determined by the developer. These containers while opaque to the operating system are managed by the OS. This paper analyzes the threats and attacks to applications. It then describes the ISA extension for generating a HW based container. Finally it describes the programming model of this container.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

Copyright is held by the owner/author(s).

HASP '13, Jun 23-24 2013, Tel-Aviv, Israel  
ACM 978-1-4503-2118-1/13/06.